A publication of the DCIS Northeast Field Office

TECHNOBABBLE

The DCIS Cyber Crime Newsletter

TECHNOBABBLE
Volume 2, Issue 2

March, 2001

This issues suggested computer crime bookmarks:

@Stake's Computer Security Page:

http://www.atstake.com/security_news

The Ultimate Collection of Computer Forensic Software:

http://www.tucofs.com

Internet Service Provider Legal Contact List:

http://www.infobin.org/cfid/isplist.htm

Inside this issue:

Texas Teen Pleads Guilty to Security Breach

Nicholas Verger, a seventeen year old from Beaumont, TX, pled guilty to breach of computer security. An investigation determined that Verger illegally gained access to a Defense Information Systems Agency (DISA) computer in St. Louis, MO. Verger's intrusion specifically targeted a U.S Army procurement system and copied and transferred a highly sensitive password file. This activity caused a costly computer shutdown and subsequent repair of the system.

In November of 2000, in response to the seriousness of his crime, Verger was certified as an adult, and indicted on charges brought by the District Attorneys Office, Jefferson County, Texas. According to court records, Verger reportedly obtained a password to the web site over the Internet from a computer hacker in Florida who was previously indicted after hacking into NASA computer systems. Defense Department special agents were able to trace the unauthorized access to the telephone line in Verger's Beaumont home. It was discovered that Verger had also gained access to a NASA web site

The case was originally turned over for prosecution to the U.S. Attorney's office, but Verger could not be tried as an adult in federal court. Assistant U.S. Attorney John Stevens said a juvenile can be tried as an adult for drug or weapons offenses or for especially violent crimes. Legislation might be filed to address what Stevens called "this glitch in the law."

"We're finding that young people are more sophisticated in computer-related crimes," he said.

Verger was 16 at the time of the alleged offense last Dec. 14. The indictment charges that the breach of computer security cost $3,000 for government technology experts to repair.

Something serious like this needs to be dealt with to send a message," Stevens said.

The investigation was conducted by the Defense Criminal Investigative Service, the National Aeronautics and Space Administration's Office of the Inspector General - Computer Crime Section, and the Federal Bureau of Investigation.

Document Fraudster Allegedly Used Internet

Ivan G. Beaulieu was sentenced in U.S. District Court, Cleveland, OH, to 51 months incarceration, followed by 2 years supervised release, and a $300 special assessment. Beaulieu previously pled guilty to possession of forged securities of the States and private entities, one count of fraud and related activity in connection with identification documents, and one count of sale or receipt of stolen vehicles. An investigation was initiated when information was received that Beaulieu had manufactured and sold counterfeit Department of Defense facility identifications, as well as DEA special agent credentials. When arrested by the Ohio State Highway Patrol near Cleveland, OH, Beaulieu was also in possession of 370 counterfeit checks.

A review of the forged instruments has led investigators to believe that the high quality forgeries were created utilizing images and graphics readily available on the Internet, in conjunction with a high quality printer, and laminating devices.

The investigation was conducted by the Defense Criminal Investigative Service, the U.S. Secret Service, the Drug Enforcement Administration, and the Ohio State Highway Patrol.

Input Validation Attacks

In the world of computer hacking, many system vulnerabilities fall into a category which can be exploited via a method know as an Input Validation Attack, or IVA.

IVA's DEFINED:

Each and every day, you utilize various programs which require input— programs as simple as a calculator, to the most advanced web browsers — require input from users. These programs utilize complex source code instructions which, in turn, determine how the information which has been input into your system is to be treated. So, what happens when programming errors cause a program to incorrectly validate the input that you give it ?

All too often, the results can be disastrous. Suppose, for example, a certain Internet based application you are utilizing requires you to type a password of a certain length. You input a password several characters longer than that which is allowed. If the program's source code does not know how to effectively deal with the extra characters (generally, the proper response would be to ignore them), one of several things could happen:

1) The program may lock up, and make your system completely inaccessible.

2) The program will continue to run without any noticeable flaws.

3) The program may become confused, and terminate due to its inability to deal with the extraneous data.

HACKING USING IVA's

So, assuming this type of programming bug exists, and the program doesn't make sure that correct input is given, how can a hacker use this fact to his or her advantage? One of the most serious consequences that can be taken advantage of lies in the fact that when certain programs are running in memory, they require access to certain system resources / information that wouldn't generally be accessible to the typical user. For example, when a user initially logs into a computer system by providing a password, the password application may have to temporarily allow the user's system to access a password validation list that could typically only be accessed by a system administrator (root level user, or "superuser"). If the user could take advantage of an Input Validation error within such a program, he or she may force a system crash while the program is executing. If the crash causes program termination, the user could purposely attach extraneous information to the data that is input, and thus force the program to "shell out" to a command prompt (the flashing cursor that appears when a computer is waiting for system input). If the IV bug causes the program to crash during the period of time that system privileges were temporarily escalated, the user could find themselves staring at a command prompt with root level privileges. At this point, the user would effectively "own" the system at issue. He or she would have the ability to change the system in any way, shape, or form, including accessing any and all data on the system, deleting all information on the system, creating new user accounts for subsequent use, etc.

PREDOMINANCE OF IVA's

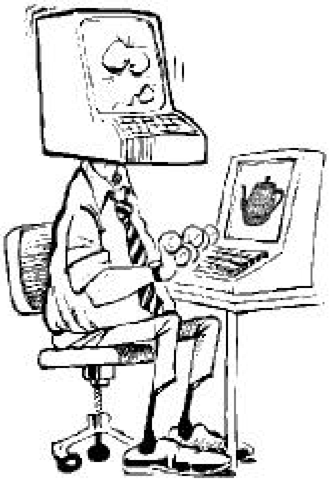
So, you may ask, what are the odds that hackers could scrutinize code to extent that they could find these programming bugs that could potentially allow them to take over systems? To date, hackers have been incredibly successful, due in large part to the open source nature of source code utilized within systems such as Linux. Microsoft, which protects its source code from public release, has not been exposed to the constant barrage of IVA's that the Linux community has seen as of late.

HOW TO PREVENT IVA's

1) Make sure that daemons function with privileges that are as restrictive as possible, and can only access files that they should have access to (i.e. a web server needs to be able to read certain files, but may not require write access.

2) Make sure you check CERT postings regularly for latest IVA discoveries, and utilize patches promptly. Many Input Validation attacks being utilized have been publicized for quite some time, but lack of vigilance on the part of administrators has resulted in systems not being updated as promptly as they should be.

3) Developers must take security into mind when coding programs, and test them under unexpected conditions. Until this is accomplished across the board, we can expect to see IVA's rear their ugly heads time and time again.



"Developers must take security into mind when coding programs, and test them under unexpected conditions. Until this is accomplished across the board, we can expect to see IVA's rear their ugly heads time and time again."

Alleged FBY Spy Sought Anti-Hacking Position

"Hanssen twice aggressively expressed an interest to Invicta executives on being employed by Invicta following his retirement from the FBI"

Accused FBI turncoat Robert Hanssen wanted to retire into a job selling anti-hacker technology to the government — to guard against double agents — a former CIA director said recently.

James Woolsey, who led the CIA under former President Bill Clinton, said Hanssen pushed for a job with Invicta Networks, a firm founded by Soviet KGB defector Viktor Sheymov to develop hack-proof computer software for U.S. spy agencies.

"Hanssen twice aggressively expressed an interest to Invicta executives on being employed by Invicta following his retirement from the FBI," said Woolsey, who is on Invicta's board and also serves as Sheymov's attorney.

Hanssen, who allegedly used his computer expertise to hack into FBI files for secrets to sell to Moscow, also boasted to FBI colleagues about getting a big-bucks job when he retired, according to an FBI affidavit.

In February 1988, Hanssen allegedly told his Soviet handlers that he could read the FBI'S files on Sheymov's debriefings, the affidavit said. More recently, "Hanssen told FBI co-workers that he was considering an offer of lucrative employment by Sheymov after retirement in April," the affidavit said.

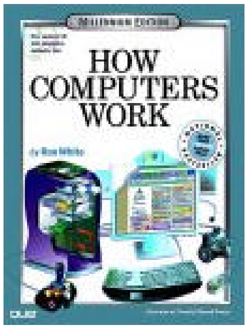
Three weeks before he was arrested, Hanssen "was allegedly briefed on the Invicta technology" as part of his official duties along with several other FBI computer experts, Woolsey said.

Sheymov was a rising star and the youngest major in the KGB at age 33 when he defected to the U.S. in 1980 with his wife and daughter. His defection was considered one of the CIA's major Cold War coups.

Hanssen, 56, has been charged with espionage crimes carrying the death penalty for allegedly selling secrets to the Soviets and later the Russians for at least $1.4 million in 15 years as a mole.

This Issues Suggested Reading

How Computers Work



This issues suggested reading is "How Computers Work," by Ron White.

Why would a computer crime investigator require an introductory text such as "How Computers Work?" A quick glance through Ron White's thorough text will reveal that it is much more than just a simple computer primer.

White effectively succeeds in an area that computer crime investigators are all too often found lacking—namely, the ability to explain complex technical details in a manner that can be understood by laymen. White also makes very good use of visual aids in simplifying descriptions of complex hardware and processes. The text will assist investigators in developing clear explanations of technical issues which are free of jargon and distraction. As any investigator realizes, this ability can oftentimes make the difference between successful presentation of a case to jurors, or failure to effectively relay information.

A recent Amazon.com editorial review sums the book up nicely when it states, "Will it help you get more work done with your computer? No. Will it enable you to do things you couldn't do before? No. Rather, *How Computers Work* will help you understand in a broad sense what's going on when you tap the keys, click the mouse, and set software to work. Reading White's sharp prose won't make you qualified to work as a computer repair technician. This book will, however, make you a more informed computer user. You'll have a better idea of what's going on inside the beige enclosure."

Title:
How Computers Work

Author:
Ron White

Cost: **$29.99**

ISBN: **0-7897-2112-0**

Publisher: **QUE**

This Issue's Useful Definition

Viruses and How They Work

Nowadays, the discovery of new computer viruses, or derivatives of previously released viruses, is a daily occurrence. But how many people truly understand what a virus is, and how viruses work?

Simply put, a virus is defined as **a program intentionally designed to associate itself with another program—so that when that program is executed, the virus is also executed, and then replicates itself by attaching itself to other programs.** Many are also designed to deliver a destructive result upon execution, such as deleting files, or modifying data. What makes viruses different from other malicious code, such a trojan horses, or logic bombs, is the fact that viruses are specifically designed to replicate themselves so that the destructive results can be spread amongst other users.

Viruses generally take the following actions once they are executed:

1) The virus copies itself to program files, or a hard disk's or floppy disk's master boot record.

2) Many viruses will then look for executable files that can be "infected." The virus will insert malicious code behind a small section of code at the beginning of the file known as the file header (this header contains simple information defining the type of file). This results in the malicious code being executed prior to the file's true code.

3) Other viruses will avoid executables, and attach themselves to the master boot record of a disk. Computers access the MBR on a regular basis, which assures that the malicious code will be executed, perhaps time and time again.

4) When the virus is actually executed, it may begin monitoring the system… and waiting until specific events occur. The virus will then respond in kind once an action occurs. For example, the virus may wait for a specific date, and then delete all files on a computer's hard disk. Or it may wait for a user to assign an attachment to an e-mail, and respond by infecting the attachment so that it can deliver malicious code to other users.

The actual impact of viruses can vary greatly. Many viruses have been discovered that are actually quite innocuous. Some simply inform a user that their system has been infected, and perform no subsequent action. Others may make random changes to various text files that it can locate on the infected system's hard drive. Still others may force the computer into an "endless loop," whereby the system's processing power is degraded by virtue of the fact that the malicious code is forcing the system to complete endless computations. While many viruses are created to impact a system immediately, others can lurk within a system for days, months, and even years… waiting for the perfect set of circumstances prior to announcing its presence. Noteworthy is the fact that viruses are also becoming more and more complex and "stealth-like." In fact, many new viruses are created so that they not only replicate themselves, but actually modify themselves each time replication takes place so as to avoid detection.

VIRUS DETECTION

Antivirus software generally function in one of two manners. **Signature scanners** compare contents of master boot records and files located on disks with sections of code specific to certain viruses. If the signatures match, it is assumed your system is impacted by a previously discovered virus. Unfortunately, this method works only with viruses that have already been analyzed. On the other hand, **Heuristic Detectors** explore code and look for events which are triggered by time and date routines, and disk routines that bypass an operating system. Both signature scanners and heuristic detectors have their strong and weak points, but both rely upon the user performing upgrades or downloading updates on a regular basis to ensure that new viruses will be identified.

> *"A virus is defined as a program intentionally designed to associate itself with another program—so that when that program is executed, the virus is also executed, and then replicates itself by attaching itself to other programs."*

Virus History Timeline

1986	**The first PC virus—known as the 'Brain' virus– written in Pakistan.**
1988	**'Cascade' virus found in Europe. The first anti-virus software developed.**
1989	**'Datacrime, Dark Avenger, and Frodo viruses unleashed.**
1992	**Media mayhem ensues with the release of 'Michaelangelo.'**
1995	**Anti-virus companies fear that release of Windows 95 may eliminate viruses. Macro viruses soon prove them wrong.**
1999	**'Melissa' macro virus uses MS Word & Outlook to infect incredible number of system. Causes millions in damages.**
2000	**'I Love You' virus transmitted to all on users address books. Like Melissa, Causes millions in damage.**
2001	**Kournikova virus uses men's primal urges against them!**

CIA Utilizing Data Mining Techniques

The Central Intelligence Agency is reportedly using data mining technology to find useful information within documents and broadcasts in different languages.   On a daily basis, the agency sifts through an incredible amount of information from both classified and unclassified sources in varied formats such as hard text, digital text, imagery, and audio in more than 35 languages.

The CIA's Directorate of Science and Technology is reportedly focused on finding solutions to the challenge of sifting through such voluminous data.

``We're not growing at a fast rate, but the amount of information that comes into this place is growing by leaps and bounds," Larry Fairchild, a CIA representative said in an interview. The agency is exploring how to "give folks technologies so that they are able to handle the big increase in information they're going to have to deal with on a day-to-day basis."

One computer tool called ``Oasis" can apparently convert audio signals from television and radio broadcasts into text. It can distinguish accented English for greater accuracy in the transcription, whether the speaker is male or female, and whether one male or female voice is different from another of the same gender.

If one voice is labeled with a name, the computer from then on will put that name on anything else with that same voice. So for example if a broadcast by Saudi-exile Osama bin Laden, whom the CIA considers a major threat to Americans, was transcribed and labeled, every time his voice was detected the computer would automatically label it.

COMPUTER TRANSLATION

If the computer's translation appears incorrect, an operator can choose to hear the actual broadcast. For example, the demonstration showed a transcription that read ``latest danger from hell" but the audio said ``latest danger from el nino."

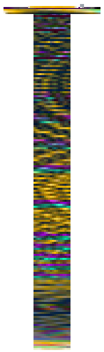
The computer cuts down on the time it would take a person to transcribe a half-hour broadcast to 10 minutes from up to 90 minutes, a CIA employee conducting the demonstration said. The CIA is planning to have Oasis developed for different languages such as Arabic and Chinese.

It also finds similar meanings of words being searched, for example a broadcast might not mention ``terrorism" but might say "car bombing," which the computer would tag as ``terrorism" so that anyone searching for that category would find it. Currently the CIA's Foreign Broadcast Information Service is using it in one Asian city and intends to have it in other regions such as the Middle East this year.

Another computer tool known as `FLUENT," enables a user to conduct computer searches of documents that are in a language the user does not understand.   The user can put English words into the search field, such as "nuclear weapons," and documents in languages such as Russian, Chinese and Arabic pop up. The system will then translate the document and if it is seen as useful, the analyst can send it to a human translator for more precision.

Languages that FLUENT can translate into English include Chinese, Korean, Portuguese, Russian, Serbo-Croatian and Ukrainian.

``Data mining" tools are used to extract key pieces of information from a variety of intelligence traffic such as on the flow of illegal drugs and also to keep track of illicit financial transactions.



Tools were developed to help CIA analysts on Iraq, who were asked to analyze the agency's holdings on Iraqi war crime violations, about 1.2 million documents going back to 1979. The Text Data Mining tool extracted and indexed all words in the data so for example if an analyst was asked whether Iraq ever used anthrax as a weapon, the analyst could open the tool and find anthrax in the automatically generated index. That tool also counts the frequency of word use and can handle various spellings of the same Iraqi names or locations.

``We're not growing at a fast rate, but the amount of information that comes into this place is growing by leaps and bounds," - Larry Fairchild, CIA representative.

There is also ``gifting technology" which gives the flavor of the key information of a document in a short paragraph, Fairchild said.

With the latest spy furor in the nation's capital, would any of the tools help catch a spy? ``Yes, some of the things we're doing can," Fairchild said without details. ``We're looking at better technologies to put in that area," he added.

For more on the CIA's Directorate of Science and Technology, check out their website at :

http://www.cia.gov/cia/dst/index.html

A publication of the DCIS Northeast Field Office

Defense Criminal Investigative Service
Northeast Field Office
10 Industrial Highway, Bldg. G, Mail Stop 75
Lester, PA 19113

Phone: (610) 595-1900
Fax: (610) 595-1934

Send comments to: Jives@dodig.osd.mil

We're on the Web!
www.dodig.osd.mil/dcis/dcismain.html

The Defense Criminal Investigative Service

"Protecting America's War Fighters"

The Defense Criminal Investigative Service is the investigative arm of the U.S. Department of Defense, Office of the Inspector General. As such, DCIS investigates criminal, civil, and administrative violations impacting the Defense Department. Typically, DCIS investigations focus upon computer crime involving U.S. military and civilian DoD systems, contract procurement fraud, bribery and corruption, health care fraud, anti-trust investigations, export enforcement violations, environmental violations, and other issues that impact the integrity and effectiveness of the U.S. Department of Defense.

If you encounter issues that impact the U.S. Department of Defense, please call the DCIS office within your region.

DCIS Northeast Field Office.
10 Industrial Hwy., Bldg. G
Lester, PA 19113
Phone: (610) 595-1900
Fax: (610) 595-1934

DCIS Boston Resident Agency
Rm. 327, 495 Summer Street
Boston, MA 02210
Phone: (617) 753-3044
Fax: (617) 753-4284

DCIS Hartford Resident Agency
525 Brook Street, Suite 205
Rocky Hill, CT 06067
Phone: (860) 721-7751
Fax: (860) 721-6327

DCIS New Jersey Resident Agency
Wick Plaza 1, 100 Dey Pl., Ste. 102
Edison, NJ 08817
Phone: (732) 819-8455
Fax: (732) 819-9430

DCIS New York Resident Agency
One Huntington Quad, Suite 2C01
Melville, NY 11747
Phone: (516) 420-4302
Fax: (516) 420-4316

DCIS Pittsburgh Post of Duty
1000 Liberty Ave., Ste. 1310
Pittsburgh, PA 15222
Phone: (412) 395-6931
Fax: (412) 395-4557

DCIS Syracuse Resident Agency
441 S. Selina St., Ste. 304
Syracuse, NY 13202
Phone: (315) 423-5019
Fax: (315) 423-5099